Praktikum 4

*Lapisan Transport*

# Lab 4.5.1: Mengamati TCP dan UDP Menggunakan Netstat

## Tujuan

* Menjelaskan paarmeter perintah netstat dan keluarannya.
* Menggunakan netstat untuk mengamati informasi protokol pada komputer.

## Latar Belakang

Perangkat utilitas netstat merupakan singkatan dari network statistics, tersedia luas pada komputer Windows dan Unix / Linux . Dengan mengaplikasikan opsi-opsi pada perintah akan menghasilkan keluaran yang berbeda. Netstat menampilkan koneksi jaringan yang masuk dan keluar (TCP dan UDP), informasi tabel routing, dan statistik antarmuka.

## Skenario

Pada praktikum ini, mahasiswa menggunakan perintah dan mengaplikasikan opsi-opsi untuk menganalisa dan memahami status protokol Lapisan Transport TCP/IP.

## Tugas 1: Menjelaskan parameter opsi-opsi netstat dan keluarannya.

Buka jendela Terminal dengan mengklik Start | Run. Ketik cmd, dan tekan OK. Untuk menampilkan informais help mengenai perintah netstat gunakan opsi /? options, sebagaiman ditunjukkan pada perintah berikut :

**C:\> netstat /?** <ENTER>

Dengan menggunakan perintah **netstat /?** pada jendela terminal, **Tuliskan opsi-opsi beserta deskripsi keluarannya ! (minimal 5 opsi)**

|  |  |
| --- | --- |
| Opsi | Deskripsi Keluaran |
|  |  |
|  |  |

Ketika statistic **netstat** menampilkan koneksi TCP, maka pada kolom terakhir tertera status TCP. Serangkaian status TCP ditampilkan selama sesi koneksi TCP. **Sebutkan dan**

### jelaskan status-status TCP minimal enam ! (Untuk menjawab pertanyaan ini, silahkan unduh dokumen RFC 793)

|  |  |
| --- | --- |
| Status | Deskripsi Koneksi |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Alamat IP pada netstat terbagi atas kategori :

|  |  |
| --- | --- |
| Alamat IP | Deskripsi |
| 127.0.0.1 | Alamat ini mengacu pada localhost |
| 0.0.0.0 | Alamat global yang berarti “ANY” |
| Remote Address | Alamat perangkat remote yang terkoneksi dengan computer local |

## Tugas 2 : Menggunakan netstat untuk mengamati informasi protocol

### Langkah 1 : Menggunakan netstat untuk menampilkan koneksi yang aktif

Dari jendela terminal Tugas 1, jalankan perintah berikut :

C:\Users\ayah>netstat –a

**Tuliskan keluaran perintah di atas tersebut dalam bentuk table, yang terdiri atas *Protocol* (TCP dan UDP), *Local address*, *foreign address*, dan *state* ! (minimal lima TCP dan lima UDP)**

Opsi –n memaksa netstat untuk menampilkan keluaran dalam format raw. Masih dari jendela terminal yang sama jalankan perintah berikut :

C:\Users\ayah>netstat –an

**Tuliskan keluaran perintah di atas tersebut dalam bentuk table, yang terdiri atas *Protocol* (TCP dan UDP), *Local address*, *foreign address*, dan *state* ! (minimal lima TCP dan lima UDP)**

Mengacu pada keluara dari perintah netstat -n, seorang teknisi jaringan menduga bahwa computer telah diserang oleh cracker pada port 1521 dan 49158. Sebagai seorang supervisor teknisi jaringan, bagaimana analisa Anda terhadap keluaran perintah tersebut

?

C:\Users\ayah>netstat –n Active Connections

|  |  |  |
| --- | --- | --- |
| Proto Local Address | Foreign Address | State |
| TCP 127.0.0.1:1521 | 127.0.0.1:49158 | ESTABLISHED |
| TCP 127.0.0.1:49158 | 127.0.0.1:1521 | ESTABLISHED |

Jawaban : \_

### Langkah 2 : Membentuk beberapa koneksi TCP yang simultan dan menuliskan keluaran netstat

Pada langkah ini, beberapa koneksi yang simultan akan dibentuk dengan server. Perintah telnet digunakan untuk mengakses layanan jaringan pada server, kemudian mengamati protocol dengan netstat.

Buka lima jendela terminal, empat jendela terminal berukuran kecil yang digunakan untuk membentuk koneksi telnet dan satu jendela terminal yang lebih besar digunakan untuk menjalankan perintah netstat. Susun kelima jendela terminal pada layar sedemikian rupa agar semuanya dapat diamati dengan mudah dan tanpa saling menutupi.

Beberapa layanan jaringan yang dapat merespon koneksi telnet adalah sebagai berikut :

* DNS – DNS server, port 53
* FTP – FTP server, port 21
* SMTP – SMTP server, port 25
* Telnet – Telnet server, port 23

Jelaskan mengapa perintah telnet tidak dapat menggunakan protocol UDP? Jawaban :

Untuk menutup koneksi telnet, tekan tombol <CTRL> ] bersamaan, kemudian ketik quit <ENTER> untuk menutup sesi. Pada jendela terminal pertama, telnet ke server pada port 53. Pada jendela terminal kedua, telnet pada port 21. Pada jendela terminal ketiga, telnet pada port 25. Pada jendela terminal keempat, telnet pada port 23. Perintah untuk koneksi telnet ke port 53 ditunjukkan pada Gambar di bawah ini

:

C:\> telnet 10.0.0.123 53

Pada jendela terminal kelima, **catat koneksi yang terbentuk dengan perintah netstat !**

***Capture* pula setiap jendel terminal !**

## Tugas 3 : Tantangan

Tutup koneksi yang berstatus Established dengan tiba-tiba (tutup jendela terminal), dan jalankan perintah netstat –an. Amati koneksi dalam beberapa tahapan yang berbeda dari ESTABLISHED.

## Tugas 4 : Bersihkan

Jika praktikum sudah selesai, matikan computer sesuai prosedur. Rapikan kembali dan bersihkan area kerja. Pastikan tidak ada sampah dan/atau barang bawaan yang tertinggal.

# Lab 4.5.2: Protokol Lapisan Transport TCP/IP, TCP dan UDP

## Tujuan

Setelah menyelesaikan praktikum ini, mahasiswa diharapkan dapat :

* + Mengidentifikasi kolom TCP header dan cara kerjanya menggunakan Wireshark untuk menangkap sesi FTP.
  + Mengidentifikasi kolom UDP header dan cara kerjanya menggunakanWireshark untuk menangkap sesi FTP.

## Latar Belakang

Dua protocol dalam Lapisan Transport TCP/IP adalah *Transmission Control Protocol* (TCP), didefinisikan pada RFC 761, Januari 1980, dan *User Datagram Protocol* (UDP), didefinisikan pada RFC 768, Agustus 1980. Kedua protocol mendukung komunikasi lapisan yang lebih tinggi. Sebagai contoh, TCP digunakan untuk menyediakan dukungan Lapisan Transport bagi protocol FTP dan HTTP. Sedangkan UDP menyediakan dukungan Lapisan Transport bagi *Domain Name Service* (DNS) dan *Trivial File Transfer* (TFTP).

Kemampuan memahami TCP dan UDP header dan cara kerjanya adalah mutlak diperlukan bagi tenaga ahli jaringan.

## Skenario

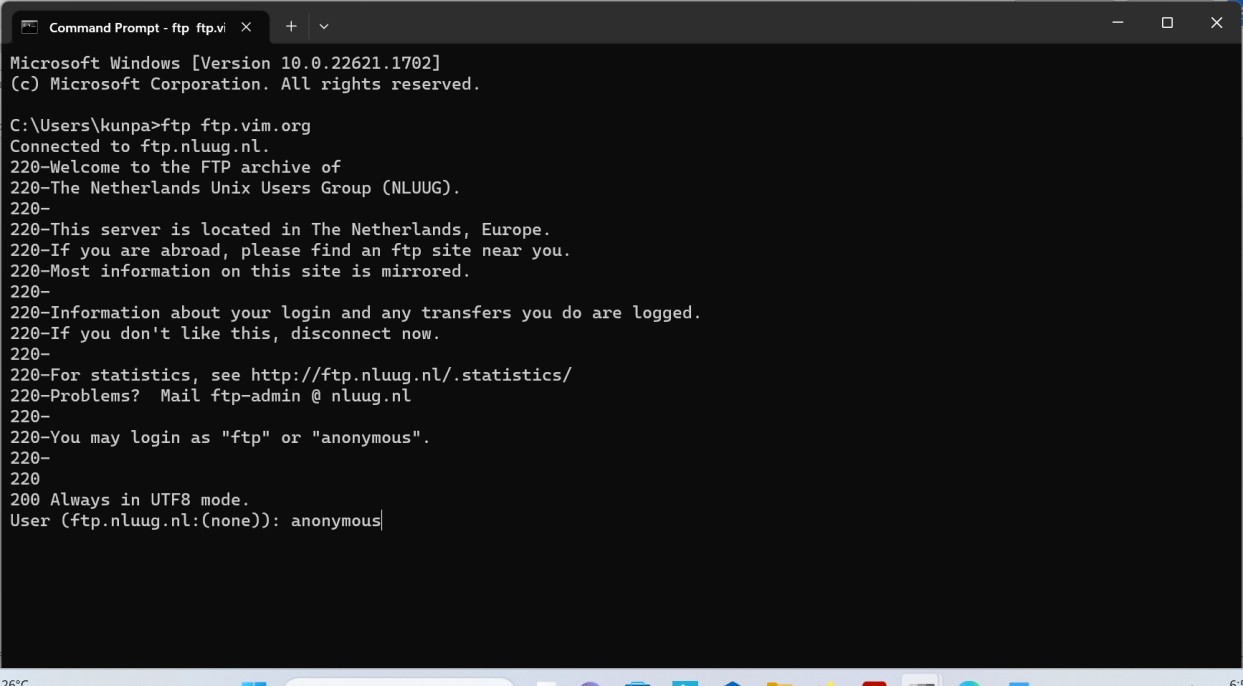
Wireshark digunakan untuk menganalisa protocol TCP dan UDP, ketika computer client mengakses dan memanfaatkan layanan FTP dan TFTP server. Selain Wireshark,pastikan aplikasi ftp dan tftp client sudah terinstall pada system operasi computer client karena khusus system operasi Windows 7 dan Windows 8, tftp harus diinstall secara manual. Untuk menginstall tftp client, klik **Control Panel > Program and Features**, pilih **Turn Windows Features On or Off**, selanjutnya centang **TFTP Client**, dan langkah terakhir klik tombol **Ok**.

## Tugas 1: Identifikasi Kolom TCP Header dan Cara Kerja Menggunakan Wireshark Untuk Menangkap Sesi FTP.

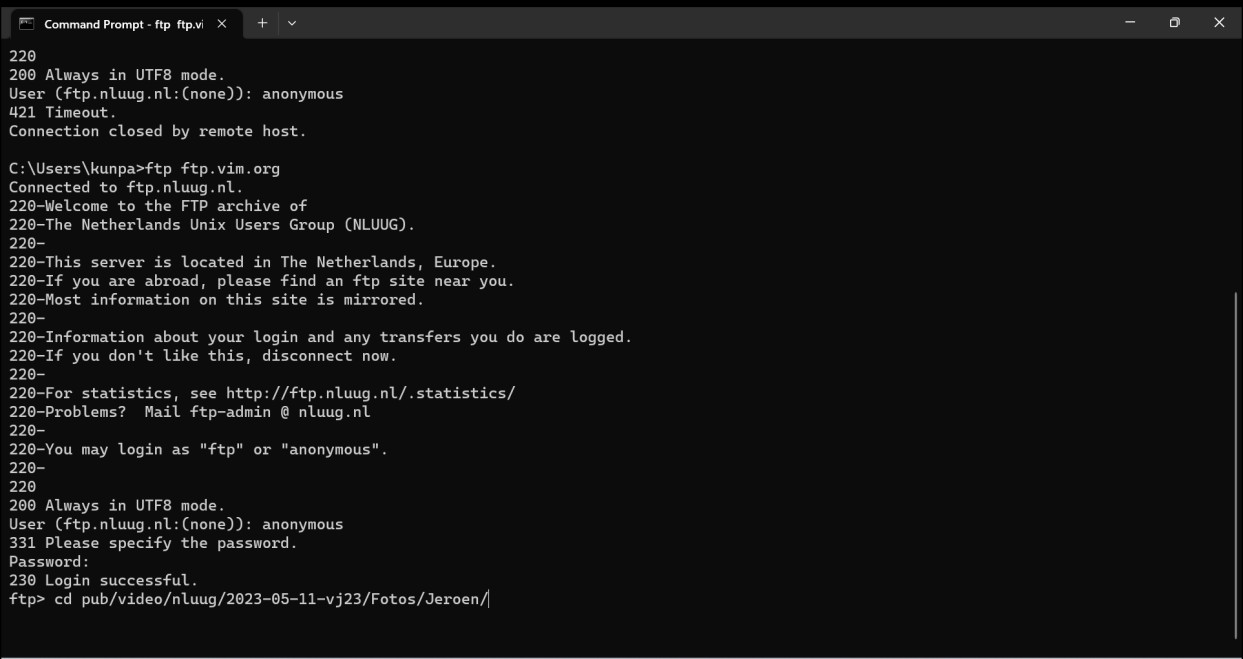
### Langkah 1: Tangkap Sesi FTP.

Sesi TCP terkendal dengan baik dan dikelola oleh pertukaran informasi pada kolom TCP header. Pada tugas ini, sesi FTP akan dibentuk ke server FTP. Setelah transfer data selesai, proses penangkapan paket dihentikan kemudian hasilnya dianalisa. Pada computer client, gunakan perintah ftp untuk mengkoneksikan ke server FTP. Setelah berhasil log in ke FTP, unduh file ke computer client.

Bagi pengguna Windows, klik **Start | Run**, ketik **cmd**, kemudian tekan **Ok**. Langkah berikutnya adalah luncurkan aplikasi Wireshark untuk menangkap paket pada antarmuka jaringan dengan alamat IP 192.168.x.y. Berikutnya adalah menjalankan perintah ftp sesuai pada Gambar 1.



Gambar 1. Login FTP

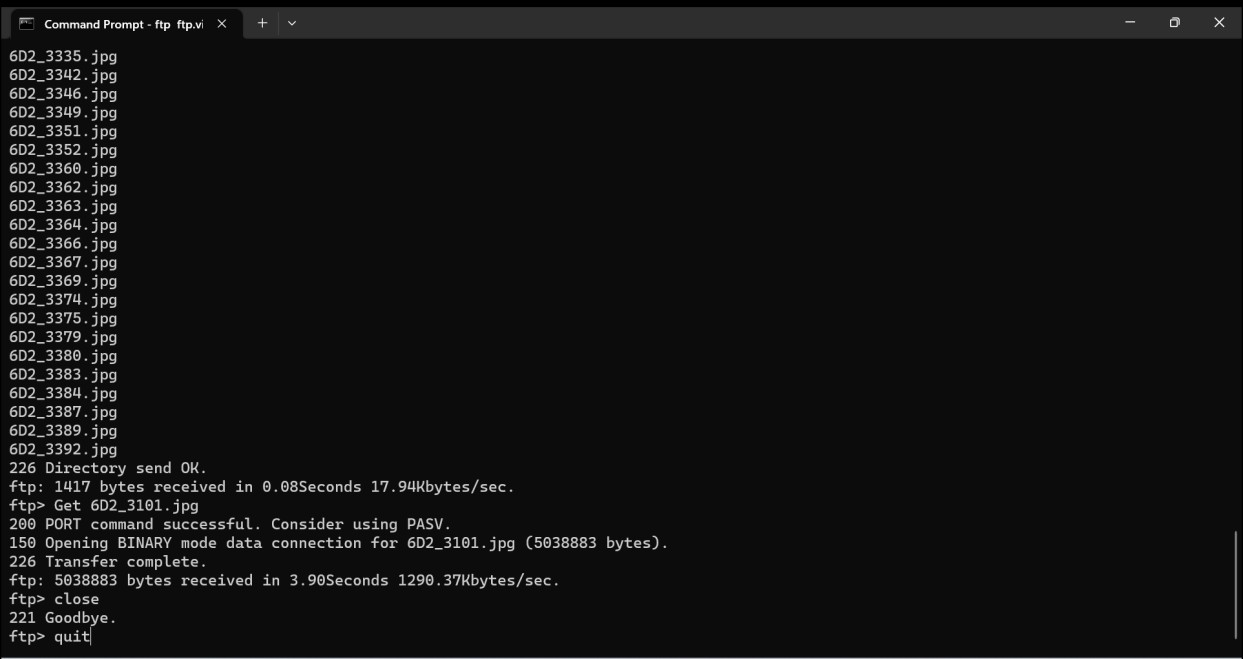
Isikan kolom user dengan **anonymous** dan password [nimkalian@mahasiswa.poliban.ac.id .](mailto:nimkalian@mahasiswa.poliban.ac.id) Pindah direktori ke **Jeroen** untuk mengunduh file **6D2\_3101.jpg**:

Gambar 2. Pindah Direktori Setelah selesai, secara berurutan jalankan perintah :

### ftp>close ftp>quit



Gambar 3. Download File



Gambar 4. Mengakhiri Sesi FTP

Langkah terakhir adalah menghentikan proses tangkapan paket Wireshark

### Langkah 2: Analisa TCP Header

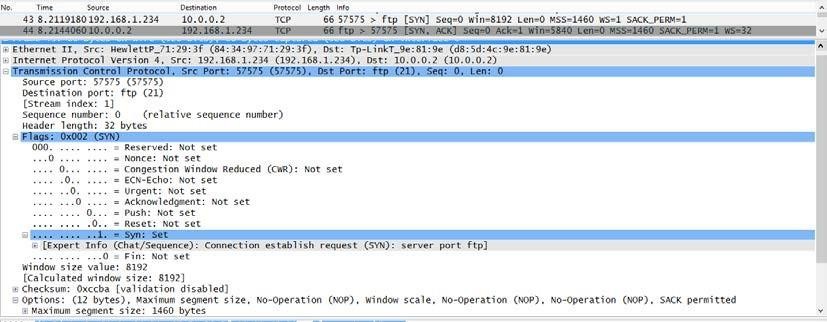
Gambar 5. Packet List Pane Sesi FTP

Beralih ke jendela hasil penangkapan paket. Jendela paling atas, yaitu Packet List Pane berisi ringkasan informasi untuk setiap lalu lintas data yang direkam. Hasil kerja mahasiswa pada Langkah 1 seharusnya sama dengan Gambar 5.

### Berdasarkan pada Packet List Pane Wireshark di masing-masing computer mahasiswa, jelaskan ringkasan informasi yang terkait dengan TCP dan FTP !

Jawaban :

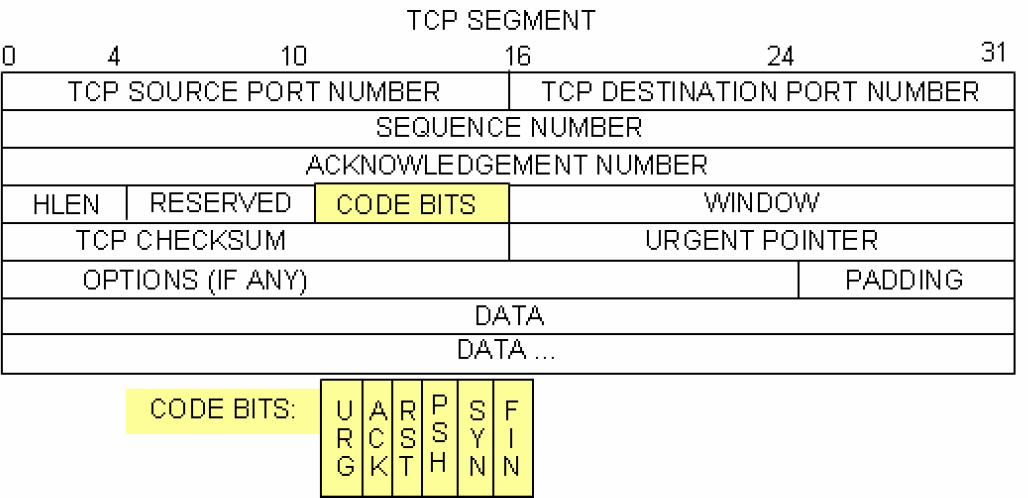
Pada wireshark, informasi mengenai TCP yang rinci tertera pada jendela tengah, yaitu Packet Detail Pane. Sorot baris pertama segmen TCP, kemudian pindahkan mouse pointer ke Packet Detail Pane. Klik tanda “+” pada Trasmission Control Protocol. Tampilan segmen TCP yang diperluas seharusnya mirip dengan Gambar 6.



Gambar 6. Segmen TCP

### Bagaimana cara mengidentifikasi segmen pertama dalam sesi TCP ?

Jawaban : \_



Gambar 7. Segmen TCP

### Berdasarkan Gambar 7, jelaskan maksud setiap *field* yang terdapat dalam segmen TCP

**!**

Jawaban : \_

Menggunakan hasil penangkapan data Wireshark, isi informasi berikut yang berkaitan dengan TCP Header !

Dari computer client ke FTP Server ( SYN bit bernilai 1)

|  |  |
| --- | --- |
| Source IP Address | … |
| Destination IP Address | … |
| Source Port Number | … |
| Destination Port Number | … |
| Sequence Number | … |
| Acknowledgment Number | … |
| Header Length | … |
| Window Size | … |

Dari FTP Server ke computer client ( ACK dan SYN bit bernilai 1)

|  |  |
| --- | --- |
| Source IP Address | … |
| Destination IP Address | … |
| Source Port Number | … |
| Destination Port Number | … |
| Sequence Number | … |

|  |  |
| --- | --- |
| Acknowledgment Number | … |
| Header Length | … |
| Window Size | … |

Dari computer client ke FTP Server (ACK bit bernilai 1)

|  |  |
| --- | --- |
| Source IP Address | … |
| Destination IP Address | … |
| Source Port Number | … |
| Destination Port Number | … |
| Sequence Number | … |
| Acknowledgment Number | … |
| Header Length | … |
| Window Size | … |

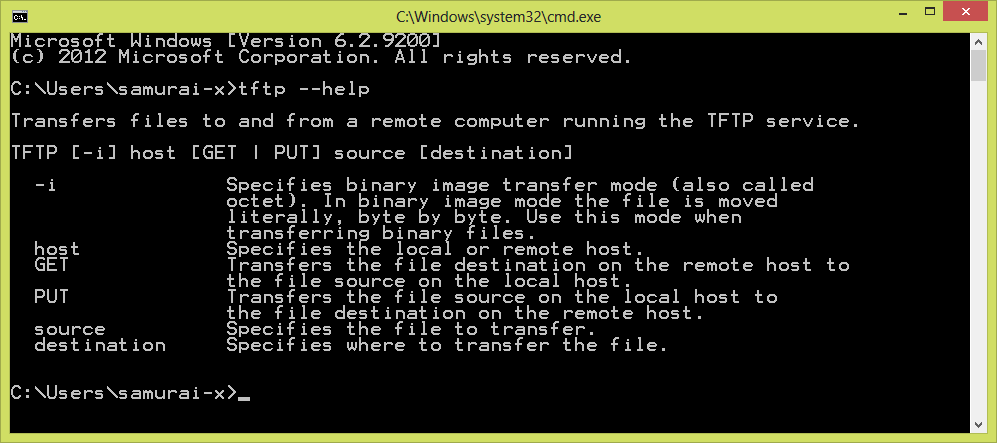
### Abaikan sesi TCP yang dimulai ketika terjadi transfer data, berapa banyak segmen TCP lainnya yang berisi bit SYN ?

Jawaban :

## Tugas 2: Mengidentifikasi Kolom UDP Header dan Cara Kerjanya Menggunakan Wireshark Untuk Menangkap Sesi TFTP.

### Langkah 1: Menangkap Sesi TFTP.

Ikuti prosedur pada Tugas 1 di atas, buka jendela terminal. Perintah TFTP memiliki sintaks yang berbeda dengan FTP, tidak ada autentifikasi. Juga, hanya ada dua perintah, yaitu get, untuk mengunduh file dan put, untuk mengirim file.



Gambar 8. TFTP Sintaks pada Window

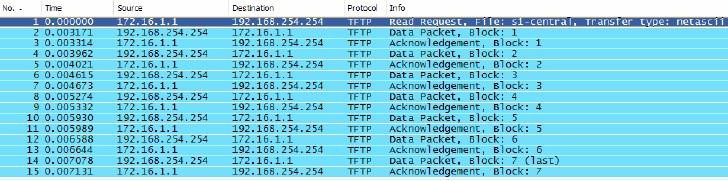
Server TFTP memiliki struktur direktori yang berbeda dengan FTP server, bahkan TFTP server juga tidak memiliki mekanisme autentifikasi.

### Tuliskan seluruh opsi tftp beserta deskripsinya!

Jawaban :

Luncurkan aplikasi Wireshark dan mulai jalankan proses tangkapan data. Lanjutkan dengan mengunduh file FuTTY.exe dari TFTP server.

### >tftp 10.0.0.123 GET winbox.exe

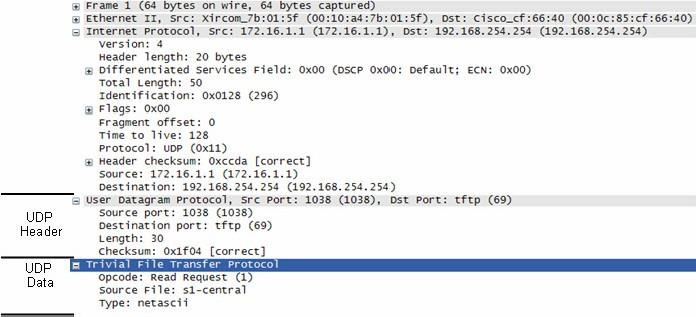
**Langkah 2: Analisa UDP *Fields***

Gambar 9. Ringkasan Sesi UDP

Beralih ke jendela *Capture* Wireshark. Hasil kerja mahasiswa pada Langkah 1 seharusnya memiliki kemiripan dengan Gambar 9.

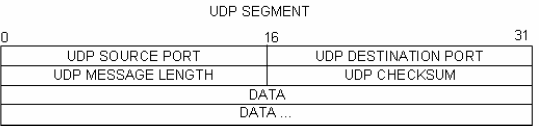
**Jelaskan apa yang dimaksud dengan *Acknowledgement* pada kolom Info ?**

Jawaban :



Gambar 10. UDP Datagram

Pada Wireshark, informasi UDP yang rinci ditampilkan pada jendela tengah atau yang disebut dengan Packet Detail Pane. Sorot datagram UDP yang pertama pada Packet List Pane, kemudian pindahkan mouse pointer ke Packet Detail Pane, klik tanda “+” pada User Datagram Protocol dan Trivial File Transfer Protocol. Tampilan datagram UDP yang diperluas seharusnya memiliki kemiripan dengan Gambar 10.



Gambar 11. Format Datagram UDP

### Berdasarkan Gambar 11, jelaskan maksud setiap field yang terdapat dalam datagram UDP !

Jawaban :\_

Dengan menggunakan hasil tangkapan Wireshark pada datagram UDP yang pertama, isi informasi berikut :

|  |  |
| --- | --- |
| Source IP Address |  |
| Destination IP Address |  |
| Source Port Number |  |
| Destination Port Number |  |
| UDP Message Length |  |
| UDP Checksum |  |

### Bagaimana cara UDP memverifikasi integritas datagram ?

Jawaban :

Amati paket pertama yang berasal dari TFTP server, isi informasi berikut yang berkenaan dengan UDP Header

|  |  |
| --- | --- |
| Source IP Address |  |
| Destination IP Address |  |
| Source Port Number |  |
| Destination Port Number |  |
| UDP Message Length |  |
| UDP Checksum |  |

## Tugas 3: Tantangan

FTP dan TFTP bukanlah protocol yang aman, semua data yang ditransfer dikirim dalam bentuk clear text. Sehingga memudahkan cracker untuk mengambil alih system. **Lakukan analisa terhadap protocol FTP dan TFTP untuk mendapatkan user id, password, dan isi file** !

## Tugas 4: Bersihkan

Hapus file yang diunduh dan yang terkait dengan hasil capture. Selanjutnya matikan computer, rapikan dan bersihkan area kerja. Pastikan tidak ada barang bawaan yang tertinggal.